IN THE UNITED STATES PATENT & TRADEMARK OFFICE

IN RE APPLICATION OF: U.S. Patent No. 7,231,040

USPTO CONFIRMATION CODE: 7212

APPLICATION NO.: 09/328,726

FILED: Oct. 26, 1998

EXAMINER: Kim Vu

GROUP ART UNIT: 2135

FOR: A MULTIPRIME RSA PUBLIC KEY CRYPTOSYSTEM

ATTORNEY DOCKET NUMBER: 200301647-6

37 CFR 1.322 & 37 CFR 1.323 REQUEST FOR CERTIFICATE OF CORRECTION

HONORABLE COMMISSIONER OF PATENTS & TRADEMARKS

Sir:

The following is a request for a certificate of correction in Serial Number 09/328,726, now Patent Number 7,231,040.

A certificate of correction under 35 USC 254 is respectfully requested in the above-identified patent.

☒ All errors were the fault of the USPTO, no fee required. In the event that a further fee is required, please charge the amount to Deposit Account No. 082025.

□ All errors were the fault of the applicant and, accordingly, please charge **$100.00** to our Deposit Account No. 082025. In the event that a further fee is required, please charge the amount to the same Deposit Account.

□ The errors were the fault of both the applicant and USPTO and, accordingly, please charge **$100.00** to our Deposit Account No. 082025. In the event that a further fee is required, please charge the amount to the same Deposit Account.

The exact locations where the errors appear in the patent and patent application are as follows:

In column 2, line 27, after “is” insert - - a - -.
(Specification filed on Oct. 26, 1998, page 4, line 5)

In column 2, line 32 (equation 6), delete “$e \cdot d \equiv 1(\mathrm{mod}(\mathrm{lcm}(p-1), (q-1))))$” and insert - - $e.d \equiv 1$ (mod(1cm((p-1), (q-1)))) - -, therefor.
(Amendment to specification filed on Oct. 2, 2000, page 1, line 5)

In column 7, line 6, above “k is the number” insert - - where $w_i = \prod_{j \neq i} p_j, and$ - -.
(Amendment to specification filed on Oct. 2, 2000, page 4, lines 1-2)

In column 10, line 39, above “Each block M” delete “$0 \leq M \leq N-1$.”
(Amendment to specification filed on Oct. 4, 2000, page 3, line 6)

In column 12, line 20, in Claim 10, after “p_2,...” delete “and”.
(Amendment to claims filed on Sep. 22, 2005, page 4, in Claim 22, line 10)

In column 13, line 49, in Claim 19, delete “steps” and insert - - step - -, therefor.
(Amendment to claims filed on Sep. 22, 2005, page 6, in Claim 27, line 2)

In column 15, line 19, in Claim 28, after “of” delete “:”.
(Amendment to claims filed on Sep. 22, 2005, page 8, in Claim 32, line 5)

In column 15, line 46, in Claim 29, after “claim 28” delete “,”.
(Amendment to claims filed on Sep. 22, 2005, page 8, in Claim 33, line 1)

In column 16, line 62, in Claim 37, delete “$M_1' \equiv C_1^{d1}(\mathrm{mod}\ p_1)$,” and insert - - $M_1' \equiv C_1^{e1}(\mathrm{mod}\ p_1)$, - - , therefor.
(Amendment to claims filed on Sep. 22, 2005, page 19, in Claim 62, line 16)

In column 16, line 64, in Claim 37, delete “$M_2' \equiv C_2^{d2}(\mathrm{mod}\ p_2)$,” and insert - - $M_2' \equiv C_2^{e2}(\mathrm{mod}\ p_2)$, - - , therefor.
(Amendment to claims filed on Sep. 22, 2005, page 19, in Claim 62, line 17)

In column 16, line 67, in Claim 37, delete “$M_k' \equiv C_k^{dk}(\mathrm{mod}\ p_k)$,” and insert - - $M_k' \equiv C_k^{ek}(\mathrm{mod}\ p_k)$, - - , therefor.
(Amendment to claims filed on Sep. 22, 2005, page 19, in Claim 62, line 20)

In column 19, line 48, in Claim 56, after “wherein” insert - - , - -.
(Amendment to claims filed on Sep. 22, 2005, page 11, in Claim 42, line 7)

In column 19, line 53, in Claim 56, after “p_2,...” insert - - , - -.
(Amendment to claims filed on Sep. 22, 2005, page 11, in Claim 42, line 10)

In column 19, line 67, in Claim 56, after "with" insert - - , - -.
(Amendment to claims filed on Sep. 22, 2005, page 11, in Claim 42, line 19)

In column 20, line 62, in Claim 64, delete "steps" and insert - - step - -, therefor.
(Amendment to claims filed on Sep. 22, 2005, page 13, in Claim 47, line 2)

In column 22, line 14, in Claim 70, delete "numbers" and insert - - number - -, therefor.
(Amendment to claims filed on Sep. 22, 2005, page 22, in Claim 86, line 2)

In column 22, line 15, in Claim 70, delete "number" and insert - - numbers - -, therefor.
(Amendment to claims filed on Sep. 22, 2005, page 22, in Claim 86, line 2)

In column 22, line 33, in Claim 73, after "p_k" insert - - , - -.
(Amendment to claims filed on Sep. 22, 2005, page 15, in Claim 52, line 9)

In column 22, line 39, in Claim 73, delete "signal" and insert - - signed - -, therefor.
(Amendment to claims filed on Sep. 22, 2005, page 15, in Claim 52, line 13)

In column 22, line 42, in Claim 73, after "with" insert - - , - -.
(Amendment to claims filed on Sep. 22, 2005, page 15, in Claim 52, line 15)

In column 22, line 60 in Claim 73, delete "$d \equiv e^{-1} \mod (p_1-1) \cdot (p_2-1) \cdot \ldots \cdot (p_k-1))$" insert - - $d \equiv e^{-1} \mod ((p_1-1) \cdot (p_2-1) \cdot \ldots \cdot (p_k-1))$ - -, therefor.
(Amendment to claims filed on Sep. 22, 2005, page 16, in Claim 52, line 3)

In column 23, line 61, in Claim 82, after "$p_2,\ldots$" insert - - , - -.
(Amendment to claims filed on Sep. 22, 2005, page 17, in Claim 57, line 7)

In column 23, line 66, in Claim 82, delete "C, whereby" and insert - - C whereby, - -, therefor:
(Amendment to claims filed on Sep. 22, 2005, page 17, in Claim 57, line 9)

In column 24, line 2, in Claim 82, delete "$d \equiv e^{-1} \mod (p_1-1) \cdot (p_2-1) \cdot \ldots \cdot (p_k-1))$" insert - - $d \equiv e^{-1} \mod ((p_1-1) \cdot (p_2-1) \cdot \ldots \cdot (p_k-1))$ - -, therefor.
(Amendment to claims filed on Sep. 22, 2005, page 17, in Claim 57, line 12)

In column 24, line 9, in Claim 82, delete "$M_1' \equiv C_1^{d1} (\mod p_1)$," and insert - - $M_1' \equiv C_1^{e1} (\mod p_1)$, - - , therefor.
(Amendment to claims filed on Sep. 22, 2005, page 17, in Claim 57, line 17)

In column 24, line 11, in Claim 82, delete "$M_2'\equiv C_2^{d2}(\mathrm{mod}\ p_2)$," and insert - - $M_2'\equiv C_2^{e2}(\mathrm{mod}\ p_2)$, - - , therefor.
(Amendment to claims filed on Sep. 22, 2005, page 17, in Claim 57, line 18)

In column 24, line 14, in Claim 82, delete "$M_k'\equiv C_k^{dk}(\mathrm{mod}\ p_k)$," and insert - - $M_k'\equiv C_k^{ck}(\mathrm{mod}\ p_k)$, - - , therefor.
(Amendment to claims filed on Sep. 22, 2005, page 17, in Claim 57, line 20)

In column 25, line 22, in Claim 91, after "p_2,..." insert - - , - -.
(Amendment to claims filed on Sep. 22, 2005, page 25, in Claim 113, line 7)

In column 26, line 9, in Claim 92, after "p_2,..." insert - - , - -.
(Amendment to claims filed on Sep. 22, 2005, page 26, in Claim 114, line 10)

In column 26, line 59, in Claim 93, delete "steps" and insert - - step - -, therefor.
(Amendment to claims filed on Sep. 22, 2005, page 27, in Claim 115, line 2)

In column 26, line 67, in Claim 93, after "p_2,..." insert - - , - -.
(Amendment to claims filed on Sep. 22, 2005, page 27, in Claim 115, line 7)

In column 27, line 33, in Claim 94, after "C" insert - - , - -.
(Amendment to claims filed on Sep. 22, 2005, page 28, in Claim 116, line 5)

In column 27, line 40, in Claim 94, after "p_2,..." delete "and".
(Amendment to claims filed on Sep. 22, 2005, page 28, in Claim 116, line 10)

In column 28, line 15, in Claim 95, after "p_2,..." insert - - , - -.
(Amendment to claims filed on Sep. 22, 2005, page 29, in Claim 117, line 7)

In column 29, line 8, in Claim 96, after "said" delete "decoding".
(Amendment to claims filed on Sep. 22, 2005, page 31, in Claim 118, line 5)

In column 29, line 14, in Claim 96, after "with" insert - - , - -.
(Amendment to claims filed on Sep. 22, 2005, page 31, in Claim 118, line 9)

In column 29, line 37, in Claim 97, delete "steps" and insert - - step - -, therefor.
(Amendment to claims filed on Sep. 22, 2005, page 31, in Claim 119, line 2)

In column 29, line 45, in Claim 97, after "p_2,..." insert - - , - -.
(Amendment to claims filed on Sep. 22, 2005, page 32, in Claim 119, line 5)

In column 30, line 21, in Claim 98, after "$p_{k,}$" insert - - k - -.
(Amendment to claims filed on Sep. 22, 2005, page 33, in Claim 120, line 8)

In column 30, line 22, in Claim 98, after "p_2,..." insert - - , - -.
(Amendment to claims filed on Sep. 22, 2005, page 33, in Claim 120, line 9)

In column 30, line 22, in Claim 98, after "$p_{k,}$" insert - - , - -.
(Amendment to claims filed on Sep. 22, 2005, page 33, in Claim 120, linc 9)

In column 30, line 31, in Claim 98, delete "of;" and insert - - of, - -, therefor.
(Amendment to claims filed on Sep. 22, 2005, page 33, in Claim 120, line 14)

In column 30, line 32, in Claim 98, after "with" insert - - , - -.
(Amendment to claims filed on Sep. 22, 2005, page 33, in Claim 120, linc 15)

In column 30, line 67, in Claim 99, after "p_2,..." insert - - , - -.
(Amendment to claims filed on Sep. 22, 2005, page 34, in Claim 121, line 7)

In column 31, line 4, in Claim 99, delete "C, whereby" and insert - - C whereby, - -, therefor.
(Amendment to claims filed on Sep. 22, 2005, page 34, in Claim 121, line 9)

In column 32, line 7, in Claim 100, after "p_2,..." insert - - , - -.
(Amendment to claims filed on Sep. 22, 2005, page 35, in Claim 122, line 9)

In column 32, line 20, in Claim 100, delete "signal" and insert - - signed - -, therefor.
(Amendment to claims filed on Sep. 22, 2005, page 35, in Claim 122, line 17)

The requested corrections are attached on Form PTO 1050.

7/14/08
DATE

Respectfully Submitted

Name: Kevin M. Hart
Registration No.: 36,823

Attorney/Agent of Record

PTO/SB/44 (04-05)
Approved for use through 04/30/2007. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

Page 1 of 5

PATENT NO : 7,231,040

APPLICATION NO. : 09/328,726

ISSUE DATE : Jun. 12, 2007

INVENTOR(S) : Thomas Collins, et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In column 2, line 27, after "is" insert - - a - -.

In column 2, line 32 (equation 6), delete "$e \cdot d \equiv 1(\mathrm{mod}(\mathrm{lcm}(p-1), (q-1))))$" and insert - - e.d ≡ 1 (mod(1cm((p-1), (q-1)))) - -, therefor.

In column 7, line 6, above "k is the number" insert - - where $w_i = \prod_{j \neq i} p_j$, *and* - -.

In column 10, line 39, above "Each block M" delete "$0 \leq M \leq N$ -1."

In column 12, line 20, in Claim 10, after "p_2,..." delete "and".

In column 13, line 49, in Claim 19, delete "steps" and insert - - step - -, therefor.

In column 15, line 19, in Claim 28, after "of" delete ":".

In column 15, line 46, in Claim 29, after "claim 28" delete ",".

In column 16, line 62, in Claim 37, delete "$M_1' \equiv C_1^{d1}$(mod p_1)," and insert - - $M_1' \equiv C_1^{e1}$(mod p_1), - - , therefor.

In column 16, line 64, in Claim 37, delete "$M_2' \equiv C_2^{d2}$(mod p_2)," and insert - - $M_2' \equiv C_2^{e2}$(mod p_2), - - , therefor.

MAILING ADDRESS OF SENDER (Please do not use customer number below):

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, Colorado 80527-2400

This collection of information is required by 37 CFR 1.322, and 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Attention Certificate of Corrections Branch, Commissioner for Patent, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

Page 2 of 5

PATENT NO : 7,231,040

APPLICATION NO. : 09/328,726

ISSUE DATE : Jun. 12, 2007

INVENTOR(S) : Thomas Collins, et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In column 16, line 67, in Claim 37, delete "$M_k' \equiv C_k^{dk}$(mod p_k)," and insert - - $M_k' \equiv C_k^{ck}$(mod p_k), - - , therefor.

In column 19, line 48, in Claim 56, after "wherein" insert - - , - -.

In column 19, line 53, in Claim 56, after "p_2,..." insert - - , - -.

In column 19, line 67, in Claim 56, after "with" insert - - , - -.

In column 20, line 62, in Claim 64, delete "steps" and insert - - step - -, therefor.

In column 22, line 14, in Claim 70, delete "numbers" and insert - - number - -, therefor.

In column 22, line 15, in Claim 70, delete "number" and insert - - numbers - -, therefor.

In column 22, line 33, in Claim 73, after "p_k" insert - - , - -.

In column 22, line 39, in Claim 73, delete "signal" and insert - - signed - -, therefor.

In column 22, line 42, in Claim 73, after "with" insert - - , - -.

MAILING ADDRESS OF SENDER (Please do not use customer number below):

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, Colorado 80527-2400

PTO/SB/44 (04-05)
Approved for use through 04/30/2007. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

Page 3 of 5

PATENT NO : 7,231,040

APPLICATION NO. : 09/328,726

ISSUE DATE : Jun. 12, 2007

INVENTOR(S) : Thomas Collins, et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In column 22, line 60 in Claim 73, delete "$d\equiv e^{-1}$ mod$(p_1-1)\cdot(p_2-1)\cdot\ldots\cdot(p_k-1))$" insert - - $d\equiv e^{-1}$ mod$((p_1-1)\cdot(p_2-1)\cdot\ldots\cdot(p_k-1))$ - -, therefor.

In column 23, line 61, in Claim 82, after "p_2,..." insert - - , - -.

In column 23, linc 66, in Claim 82, dclctc "C, whcrcby" and insert - - C whereby, - -, therefor.

In column 24, line 2, in Claim 82, delete "$d\equiv e^{-1}$ mod$(p_1-1)\cdot(p_2-1)\cdot\ldots\cdot(p_k-1))$" insert - - $d\equiv e^{-1}$ mod$((p_1-1)\cdot(p_2-1)\cdot\ldots\cdot(p_k-1))$ - -, therefor.

In column 24, line 9, in Claim 82, delete "$M_1'\equiv C_1^{d1}$(mod p_1)," and insert - - $M_1'\equiv C_1^{e1}$(mod p_1), - - , therefor.

In column 24, line 11, in Claim 82, delete "$M_2'\equiv C_2^{d2}$(mod p_2)," and insert - - $M_2'\equiv C_2^{e2}$(mod p_2), - - , therefor.

In column 24, line 14, in Claim 82, delete "$M_k'\equiv C_k^{dk}$(mod p_k)," and insert - - $M_k'\equiv C_k^{ek}$(mod p_k), - - , therefor.

In column 25, line 22, in Claim 91, after "p_2,..." insert - - , - -.

MAILING ADDRESS OF SENDER (Please do not use customer number below):

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, Colorado 80527-2400

This collection of information is required by 37 CFR 1.322, and 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Attention Certificate of Corrections Branch, Commissioner for Patent, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

Page 4 of 5

PATENT NO : 7,231,040

APPLICATION NO. : 09/328,726

ISSUE DATE : Jun. 12, 2007

INVENTOR(S) : Thomas Collins, et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In column 26, line 9, in Claim 92, after “p_2,...” insert - - , - -.

In column 26, line 59, in Claim 93, delete “steps” and insert - - step - -, therefor.

In column 26, line 67, in Claim 93, after “p_2,...” insert - - , - -.

In column 27, line 33, in Claim 94, after “C” insert - - , - -.

In column 27, line 40, in Claim 94, after “p_2,...” delete “and”.

In column 28, line 15, in Claim 95, after “p_2,...” insert - - , - -.

In column 29, line 8, in Claim 96, after “said” delete “decoding”.

In column 29, line 14, in Claim 96, after “with” insert - - , - -.

In column 29, line 37, in Claim 97, delete “steps” and insert - - step - -, therefor.

In column 29, line 45, in Claim 97, after “p_2,...” insert - - , - -.

In column 30, line 21, in Claim 98, after “p_k,” insert - - k - -.

MAILING ADDRESS OF SENDER (Please do not use customer number below):

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, Colorado 80527-2400

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

Page 5 of 5

PATENT NO : 7,231,040

APPLICATION NO. : 09/328,726

ISSUE DATE : Jun. 12, 2007

INVENTOR(S) : Thomas Collins, et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In column 30, line 22, in Claim 98, after “p_2,…” insert - - , - -.

In column 30, line 22, in Claim 98, after “$p_{k,}$” insert - - , - -.

In column 30, line 31, in Claim 98, delete “of;” and insert - - of, - -, therefor.

In column 30, line 32, in Claim 98, after “with” insert - - , - -.

In column 30, line 67, in Claim 99, after “p_2,…” insert - - , - -.

In column 31, line 4, in Claim 99, delete “C, whereby” and insert - - C whereby, - -, therefor.

In column 32, line 7, in Claim 100, after “p_2,…” insert - - , - -.

In column 32, line 20, in Claim 100, delete “signal” and insert - - signed - -, therefor.

MAILING ADDRESS OF SENDER (Please do not use customer number below):

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, Colorado 80527-2400